Security and Privacy in Smart Meters and Smart Grids

EECE 512

Konstantin Beznosov

smart meter background

- what
  - networked embedded systems
  - use state measurement circuits that can record minute- or second-level profiles of energy usage (*load profiles*)
- promise: better efficiency & reliability
  - dynamic pricing schemes
  - remote meter reading
  - improved power outage reporting
  - load curtailment in emergencies
- how:
  - self-monitoring
  - self-diagnosis
  - demand-response
  - communication
- privacy concerns due to fine-grained energy consumption data
  - monitoring the power consumption of several households to identify temporarily vacant homes and timing burglars' break-ins
  - estimating the number of residents in a household based on the frequency of power switches turned and the number of appliances simultaneously in use
  - monitoring the location of a resident inside the home based on the type of appliances being used
  - tracking eating, sleeping, and to some extent exercise habits by monitoring household appliance usage
  - identifying the TV channel or movies being watched since television power consumption changes with the image being displayed
- security concerns of integrity & authenticity of the reported data
  - underreporting energy usage or inflating the utility bills of a neighbour

Automatic Meter Reading

- autonomously collects the consumption and status data from utility meters (e.g., electric, gas, or water meters) and delivers the data to utility providers for billing or analysis purposes
- AMR Meters
  - metering engine: measures the consumption
  - Encoder-Receiver-Transmitter (ERT):
    - microprocessor & low-power radio transmitter
    - periodically reports information such as meter ID, meter reading, tamper status

from [1]

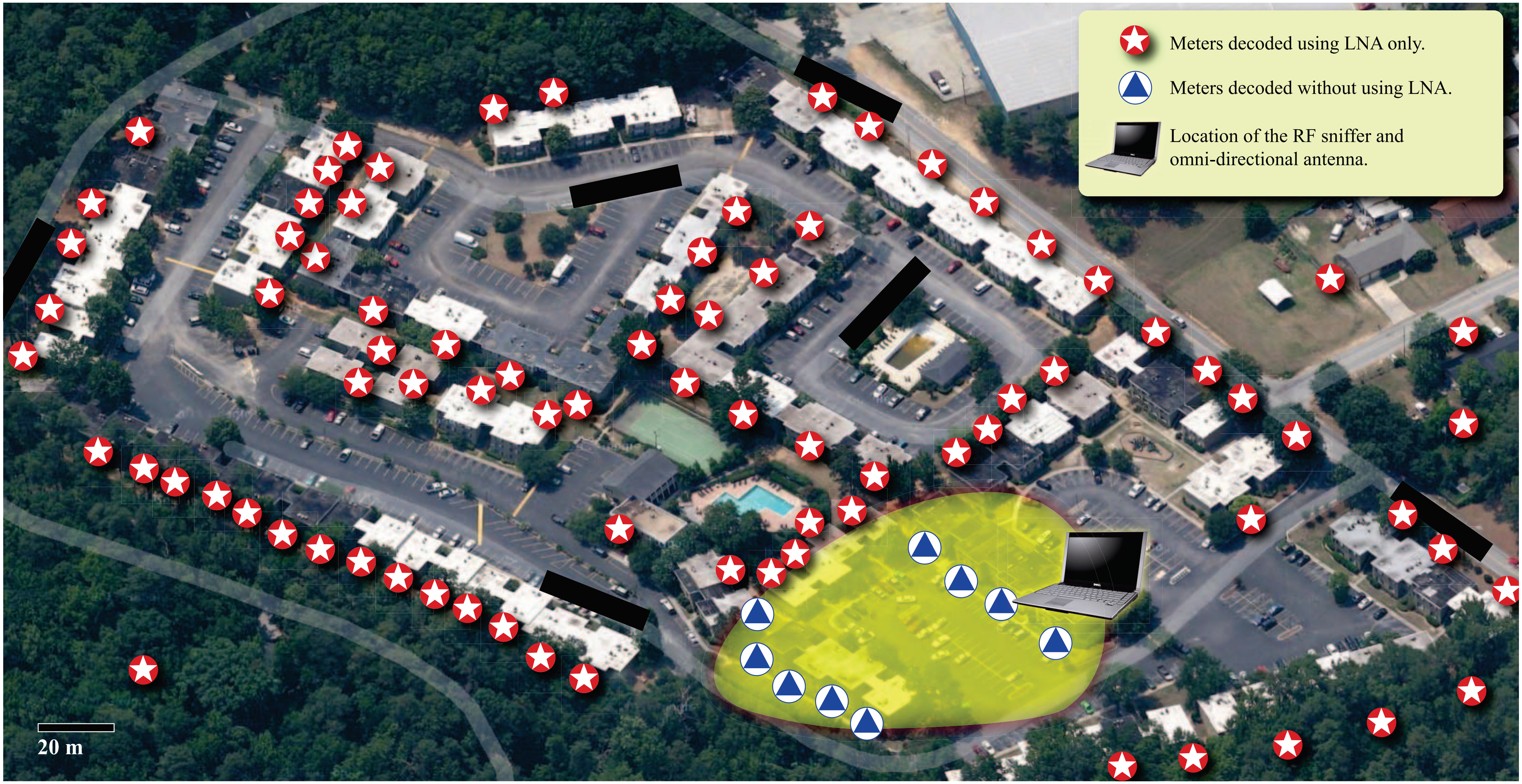
- AMR Readers:
  - handheld devices for field investigation or walk-by meter reading,
  - highly sensitive mobile collectors for drive-by meter reading,
  - a network of permanently installed collectors and repeaters for reporting AMR meter readings in real time

[1] Ishtiaq Rouf, Hossen Mustafa, Miao Xu, Wenyuan Xu, Rob Miller, and Marco Gruteser. 2012. “Neighborhood watch: security and privacy analysis of automatic meter reading systems,” In Proceedings of the 2012 ACM conference on Computer and communications security (CCS ’12). ACM, New York, NY, USA, 462-473. DOI=10.1145/2382196.2382246

reverse engineering AMR communications

- **reverse engineering requires modest effort**
  an ERT reader and programmable radio costing $1,000
- **no encryption**
  - ‘bubble- up’ meters: anyone can eavesdrop on the real time consumption of customers with meters.
  - ‘wake-up’ meters: consumption data can be eavesdropped on at arbitrary rates using activation signals
  - **battery drain attacks:** After receiving an activation signal, ‘wake-up’ meters will immediately transmit a packet
- **no authentication**
  - the ERT reader accepts any AMR transmission with a proper packet format
- **no input validation**
  - When receiving multiple packets with the same meter ID but conflicting meter readings, the ERT reader will accept the packet with the strongest signal without reporting any warning.

decoding with and without low noise amplifier


★ Meters decoded using LNA only.
▲ Meters decoded without using LNA.
Location of the RF sniffer and omni-directional antenna.
20 m

[redacted]

[redacted]

[redacted]

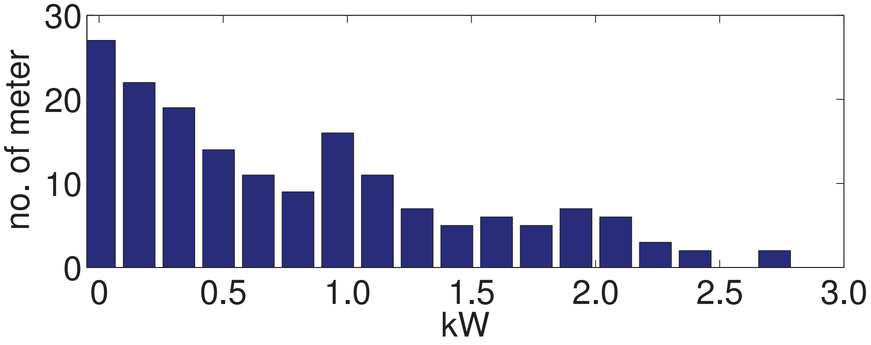
[redacted]

[redacted]

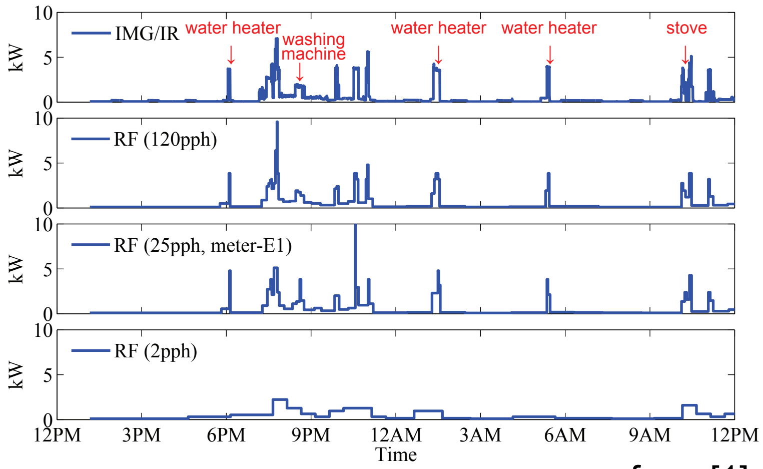
[redacted]

what can one learn from stats?

from [1]



27 meters exhibited less than 160Wh hourly power consumption



from [1]

daily routine

AMR security

- redesign the protocol
- against spoofing
  - radio fingerprinting
  - anomaly detection
  - manual checking to detect spoofing
- use ‘wake-up’ mode rather than ‘bubble-up’
  - privacy preserving jamming

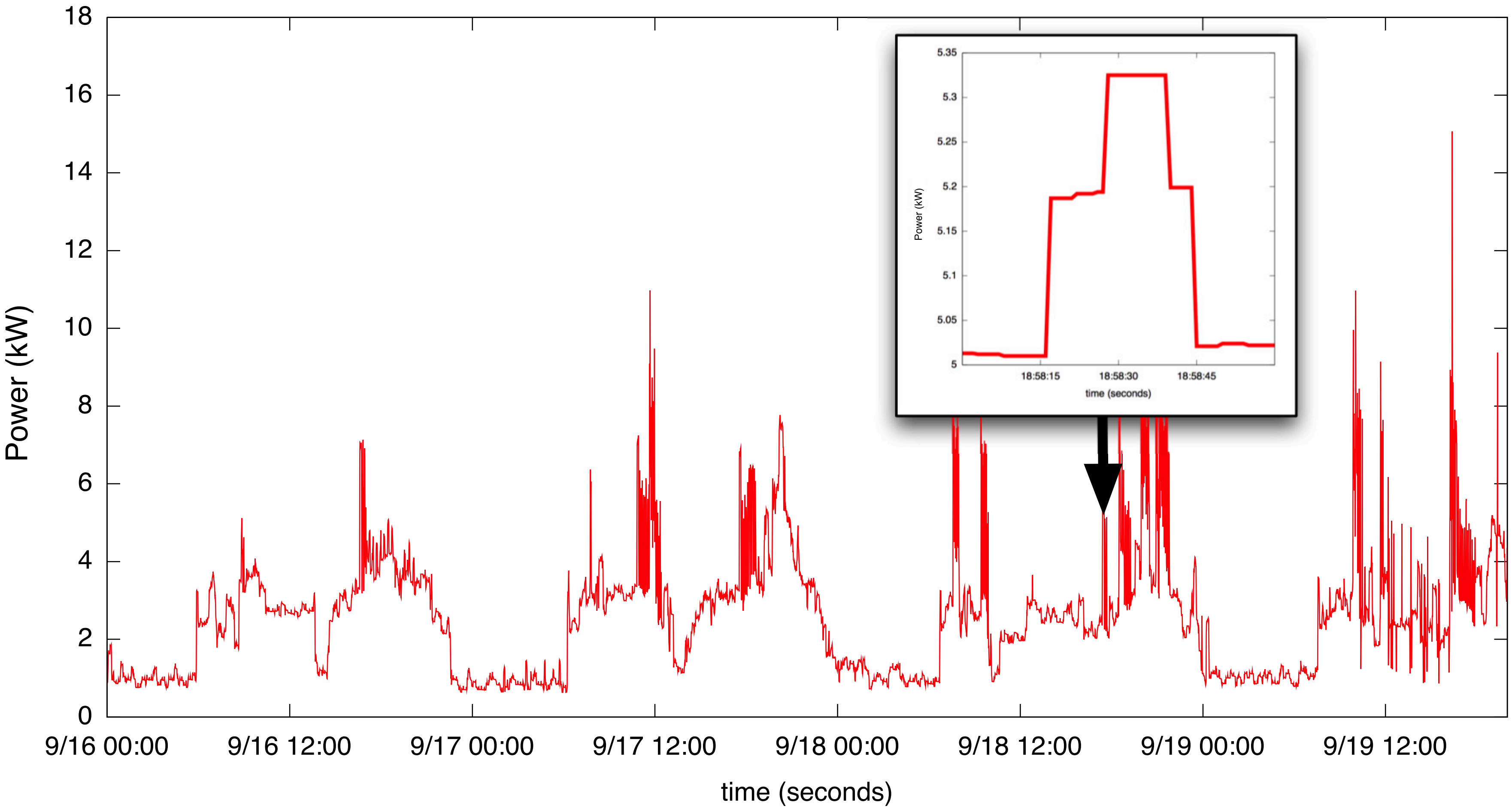
Ishtiaq Rouf, Hossen Mustafa, Miao Xu, Wenyuan Xu, Rob Miller, and Marco Gruteser. 2012. “**Neighborhood watch: security and privacy analysis of automatic meter reading systems**,” In Proceedings of the 2012 ACM conference on Computer and communications security (CCS ’12). ACM, New York, NY, USA, 462-473. DOI=10.1145/2382196.2382246

smart meters

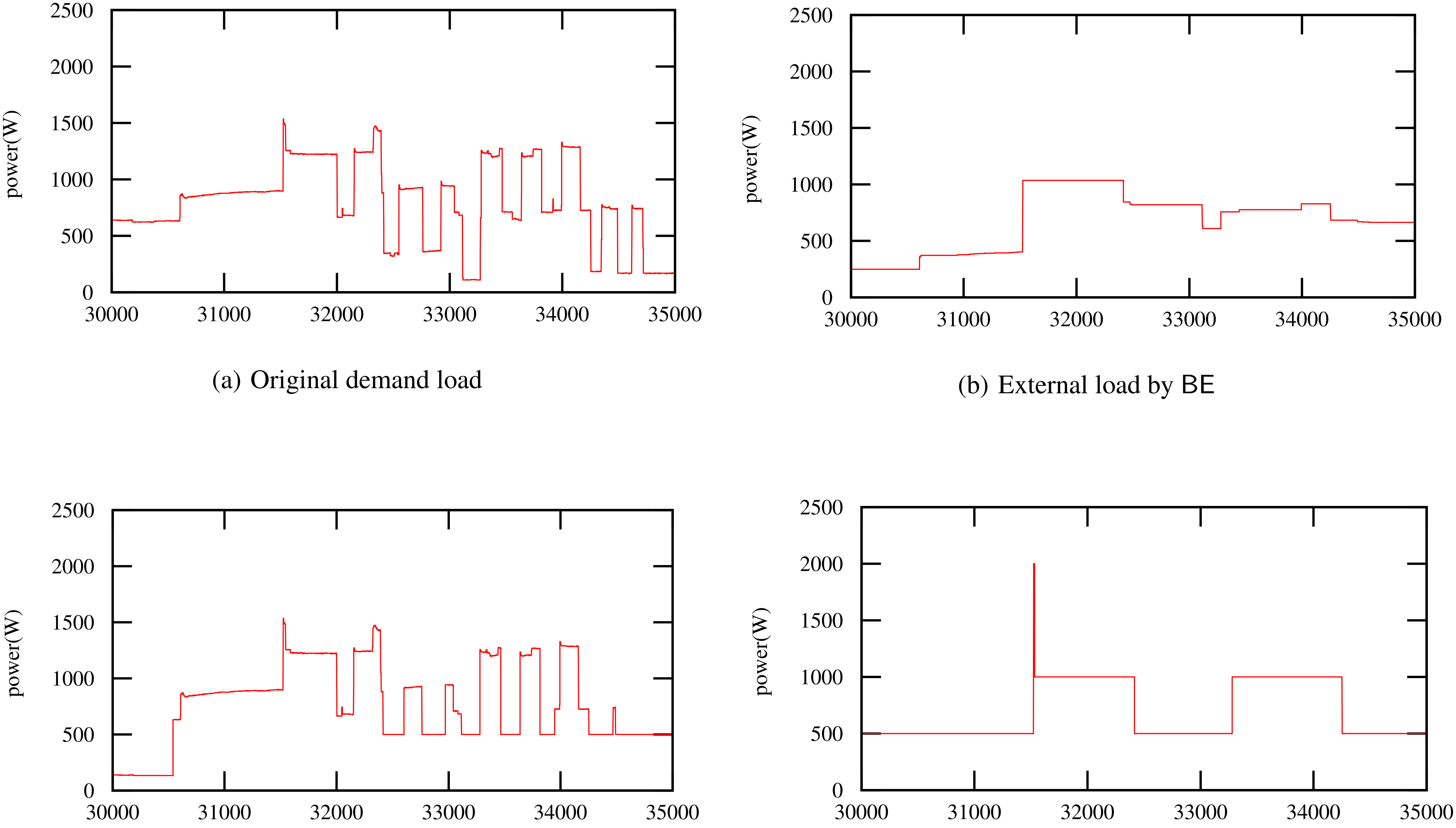
[2] Weining Yang, Ninghui Li, Yuan Qi, Wahbeh Qardaji, Stephen McLaughlin, and Patrick McDaniel. **Minimizing private data disclosures in the smart grid**. In Proceedings of the 2012 ACM conference on Computer and communications security (CCS '12). ACM, New York, NY, USA, 415-427. DOI=10.1145/2382196.2382242

risks & countermeasures

- risks
  - with Non-Intrusive Load Monitoring (NILM), load profiles can be analyzed to reveal
    - individual appliance usage
    - sleep patterns
    - number of occupants
    - times of vacancy
  - leakage to both utility companies and third parties
- countermeasures
  - Battery-based Load Hiding (BLH)
    - battery partially supplies the net demand load from the house to alter the external load
    - strategy: flatten the load profile to a constant value as often as possible


18
16
14
12
10
8
6
4
2
0
Power (kW)
9/16 00:00
9/16 12:00
9/17 00:00
9/17 12:00
9/18 00:00
9/18 12:00
9/19 00:00
9/19 12:00
time (seconds)
5.35
5.3
5.25
5.2
5.15
5.1
5.05
5
Power (kW)
18:58:15
18:58:30
18:58:45
time (seconds)

from [2]



(a) Original demand load

(b) External load by BE

(c) External load by NILL

(d) External load by LS2